3ª CONFERÊNCIA COMPUTERS PRIVACY AND DATA PROTECTION LATAM | 19-20 JULHO, 2023. | FGV, RJ - BRASIL

CPDP LatAm 2023

PROTEÇÃO DE DADOS, COOPERAÇÃO E INOVAÇÃO NA AMÉRICA LATINA

Sumário

CPDP LatAm 2023: cooperação e desafios para conseguir uma proteção de dados significativa no Brasil e na América Latina

Luca Belli, Laura Schertel, Nicolo Zingales, Walter B. Gaspar

A conferência CPDP LatAm conseguiu construir um espaço único na América Latina e no Brasil, congregando uma ampla variedade de *stakeholders* para debater perspectivas variadas e complementares a respeito da proteção de dados e seu impacto sobre a democracia, a inovação e a regulação na região.

A CPDP LatAm se tronou uma plataforma de debate multissetorial, pesquisa e capacitação reconhecida regionalmente e a edição 2023 foi dedicada à "Proteção de Dados, Cooperação e Inovação na América Latina."

O evento começou com homenagem a um dos fundadores da CPDP LatAm, o querido Danilo Doneda, ao qual é dedicado o Danilo Doneda *Award*, prêmio que destaca as melhores publicações da CPDP LatAm para honrar a memória do nosso amigo, colega e mestre, continuando nosso esforço voltado a construir juntos a cultura de proteção de dados no Brasil e na América Latina.

Como diretores do evento, neste artigo queremos compartilhar algumas reflexões sobre os avanços notáveis e os grandes desafios que permanecem ao nível latino-americano, para que a proteção de dados se torne uma realidade concreta além de um mero ideal regulatório. Assim, apesar dos avanços, estamos cientes que a integração da proteção de dados na sociedade, no desenvolvimento social, econômico e tecnológico é ainda muito incipiente, até em países vizinhos que começaram a regular o assunto há uma ou duas décadas.

No final deste artigo, o leitor poderá encontrar também a lista de todas as gravações das sessões realizadas, bem como o *Outcome Document* da CPDP LatAm 2023, que consolida os principais resultados do evento e oferece links com eventuais materiais de leitura sugeridos pelos organizadores das sessões.

Cooperar, mas como?

Um ponto de convergência ao longo de várias discussões foi a necessidade de fortalecer a coordenação e atuação multissetorial ao nível latino-americano, para enfrentar desafios comuns (reconhecimento facial, Inteligência Artificial generativa etc.), especialmente no sentido de fortalecer a coordenação das autoridades reguladoras da região.

Nenhum regulador tem um papel mais fundamental do que as autoridades de proteção de dados para orientar a evolução tecnológica baseada em coleta e processamento de quantidades enormes de dados (pessoais). Neste sentido, é necessária uma atuação conjunta e coordenada para estimular a integração da autodeterminação informacional como princípio norteador do desenvolvimento.

Cabe destacar que temos uma responsabilidade coletiva de construir essa simbiose entre inovação e proteção de dados. Como falava o artigo 1 da Lei de proteção de dados francesa, já em 1978, "A tecnologia da informação deve estar ao serviço de cada cidadão." Porém, diferentemente da região europeia, onde o desenvolvimento normativo dos últimos cinquenta anos foi acompanhado de evoluções institucionais e, particularmente, da criação de um órgão de coordenação comum, o

Comitê Europeu para a Proteção de Dados (EDPB), tal evolução institucional é ainda inexistente na região.

Contudo, é importante salientar que, apesar da clara fragmentação institucional do cenário regional, nunca foi tão "fácil" estimular uma aproximação dos marcos normativos e das autoridades reguladoras na América Latina. Sendo amplamente inspiradas no modelo europeu, as demais leis de proteção de dados da região são naturalmente compatíveis e as autoridades reguladoras estão cientes que a cooperação e a coordenação se tornaram essenciais.

As transferências internacionais de dados são um exemplo interessante de como a cooperação poderia ser particularmente benéfica, seja por meio de novos arranjos institucionais, seja por meio das cláusulas contratuais padrão, seja por meio de instrumentos de autorregulação regulada, como as cláusulas contratuais especificas, os códigos de conduta e as normas padrão corporativas que são tipicamente elaboradas por iniciativa de *stakeholders* privados, mas aprovados pelas autoridade reguladoras.

Qual inovação para fortalecer a proteção de dados?

A inovação tem um papel fundamental a desempenhar para fortalecer a proteção de dados e a privacidade. Estamos acostumados a ouvir exemplos de desenvolvimentos tecnológicos que podem prejudicar o pleno gozo da proteção de dados e enfraquecer a privacidade, mas precisamos entender que a inovação e a privacidade podem e devem ser consideradas como aliadas.

Antes de tudo, cumpre perguntar o significado da palavra "inovação", que muito frequentemente é utilizada como sinônimo de novidade. Para que uma prática seja promovida pelo sistema legal, é necessário que ela ultrapasse um certo limiar que visa a garantir sua utilidade social: assim, por exemplo, a propriedade intelectual exige cumprimento dos requisitos de originalidade, da não-obviedade e do caráter distintivo para que seja outorgada a proteção legal do direito de autor, das patentes ou das marcas, que implicam no direito exclusivo de utilização dessas invenções. Também a inovação deve se sujeitar à reflexão a respeito de sua utilidade social: qual é a inovação que promove o bem público? Como incentivá-la no contexto da governança de dados?

Em primeiro lugar, é necessário que a inovação esteja alinhada com os valores perseguidos pelo marco regulatório, razão pela qual é essencial que o regulador atue com clareza e transparência. Em segundo lugar, essa inovação pode ser promovida por pelo menos três mecanismos: (a) com incentivos reputacionais, por exemplo através da difusão de boas práticas em fóruns de discussão nacionais e internacionais, como a própria CPDP LatAm; (b) com vantagens probatórias, por exemplo, na aprovação de códigos de conduta e selos; e (c) com intervenção do governo no mercado, seja criando infraestrutura desejável (ver nesse sentido o belo trabalho feito pelo governo indiano com a arquitetura de empoderamento e proteção de dados), seja financiando atividades benéficas (como, por exemplo, as isenções fiscais oferecidas pelo PL 4/2022 para investimentos em atividades de *compliance* com a LGPD).

Ao mesmo tempo, precisamos garantir que as inovações satisfaçam necessidades sociais e não aumentem as externalidades negativas. Para isso, devemos ter muito cuidado com práticas que beneficiam uns poucos e geram prejuízos para terceiros, aumentando desigualdades que estão profundamente enraizadas em nossas sociedades. Pois, sem esses limites, o sistema de governança de dados será desconexo do bem comum e do desenvolvimento sustentável que todos os países da América Latina se comprometeram a seguir conforme a agenda ONU de 2030.

Cooperação e inovação multissetorial

Por fim, cabe frisar que quando falamos de cooperação, precisamos considerar não somente a cooperação entre reguladores e outros atores públicos, mas também o valor essencial da cooperação multissetorial. A governança *multistakeholder* não é somente algo de instrumental para proporcionar um debate mais inclusivo e para permitir uma maior qualidade no processo de elaboração normativa.

Precisamos ser inovadores também em como organizamos a nossa cooperação, seja de forma internacional, seja de forma multissetorial. As inovações tecnológicas suscetíveis de testar a resiliência da proteção de dados têm uma clara dimensão global, mas o peso e o impacto de cada *stakeholder*, tomado singularmente, é extremamente limitado.

Os acadêmicos precisamos pesquisar as soluções mais criativas, os desenvolvedores e empresários podem comercializar estas soluções para que a proteção de dados seja uma vantagem competitiva, os ativistas devem vigiar que as regras sejam respeitadas ou pedir regras mais eficientes e os reguladores devem educar e fiscalizar. Porém, se cada *stakeholder* atuar de forma isolada, será pura e simplesmente impossível definir uma agenda convergente e coerente de proteção e dados.

Uma clara mensagem que pode ser destilada da CPDP LatAm 2023 é que a cooperação já não é uma opção, é mais do que nunca uma necessidade para que as sociedades latino-americanas consigam regular o desenvolvimento tecnológico, ao invés de serem reguladas por meio de tecnologias cada dia mais difundidas.

Prefácio

A Conferência *Computers, Privacy and Data Protection* América Latina (CPDP LatAm) está se estabelecendo como uma presença notável no cenário de proteção de dados latino-americano, apesar de diferir de sua tradicional contraparte europeia. Com sua terceira edição realizada com sucesso, a conferência reuniu numerosos participantes, incluindo acadêmicos, ativistas, estudantes, representantes do governo e de organizações da sociedade civil e do setor privado. O evento, realizado no Rio de Janeiro, seguiu um formato híbrido que priorizou o envolvimento entre diversas partes interessadas, resultando na apresentação de painéis perspicazes e debates pertinentes. Esse ambiente dinâmico facilitou interações significativas, incentivando o discurso e a crítica construtiva.

Sob o tema “Proteção de dados, cooperação e inovação na América Latina”, a CPDP LatAm 2023 durou dois dias, durante os quais os participantes se debruçaram sobre várias facetas do tema. Essas discussões abrangeram uma ampla gama de tópicos, desde os desafios apresentados pela adoção de tecnologias de vigilância até a exploração da moderação automatizada de conteúdo em plataformas de mídia social. Este relatório de resultados tem como objetivo encapsular sucintamente os principais resultados de cada painel, fornecendo uma visão geral dos assuntos explorados e um resumo significativo dos resultados de pesquisa derivados desses diálogos produtivos.

A América Latina no Cenário Global de Proteção de Dados: Desafios e Oportunidades

Gravação: https://www.youtube.com/watch?v=pIMrjaBRdmY&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=8

Organização: Autoridade Nacional de Proteção de Dados

Moderação: Davi Teofilo Nunes Oliveira, ANPD

Palestrantes: Paula Vargas (Meta/WhatsApp); Jamila Venturini (Derechos Digitales);Nairane

Farias Rabelo Leitão (ANPD); Juan David Gutiérrez, (Universidad de Rosario)

- O painel debateu sobre as visões de diferentes setores (empresas, academia, sociedade civil) em relação aos desafios da proteção de dados. O palestrante Juan David Gutiérrez, integrante do setor acadêmico, propôs um debate com base nas seguintes perspectivas:
- Educação: As universidades devem ensinar sobre auditorias e conformidade; sobre o desenvolvimento de serviços a partir de metodologias de privacidade por design; e ensinar métodos de pesquisa e criação, especialmente aqueles relacionados ao "design thinking".
- Pesquisa: É importante organizar mais eventos acadêmicos nos quais se apresentem trabalhos que ampliem os horizontes de conhecimento sobre proteção de dados e privacidade. Existem agendas importantes para desenvolver sobre justiça de dados e novas governanças de coleta de dados (por exemplo, cooperativas de dados).

Antitrust, Data Protection and Privacy: What has happened so far?

Gravação:
https://www.youtube.com/watchv=1UEHUpAOLZ8&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=9

Organização: Bruno Renzetti (Insper)

Moderação: Camila Leite (IDEC)

Palestrantes: Bruno Renzetti (HK Advogados/Insper); Nicolo Zingales (FGV Direito Rio); Maria Paz Canales (Global Partners Digital); Erika Douglas (Temple University).

- O painel abordou a interação entre antitruste e proteção de dados, um tópico que esteve em destaque nos últimos anos. Os participantes discutiram os desenvolvimentos recentes na jurisprudência de diferentes países e possíveis avanços de políticas no horizonte. A decisão da Comissão Europeia no caso Meta Bundeskartellamt foi um dos principais pontos abordados pela mesa de maneira geral.
- Em particular, Renzetti e Zingales destacaram como a decisão pode motivar as autoridades no Brasil e em outros países a empregar uma nova estrutura de análise em casos de antitruste relacionados à privacidade. Erika Douglas mencionou os complementos e tensões de ambas as perspectivas de análise, enquanto Canales enfatizou a necessidade de colaboração entre as autoridades. A necessidade de desenvolver novas teorias de dano e soluções para abordar as preocupações antitruste decorrentes da privacidade no contexto do antitruste. O caso do WhatsApp foi explorado por Canales, enfatizando como a colaboração entre as autoridades na América Latina foi essencial para o sucesso da política.
- Quanto às considerações finais, os participantes foram enfáticos sobre a necessidade de promover uma maior cooperação entre as autoridades nacionais de concorrência e as autoridades de proteção de dados. Leite resumiu as discussões do painel afirmando que há uma necessidade de estabelecer um padrão de linguagem, a fim de que os diversos interessados possam entender uns aos outros.

Big data, grandes problemas: Como priorizar engajamento cívico e direitos digitais nas cidades latinoamericanas?

Gravação:
https://www.youtube.com/watch?v=VCDOiMJlqeU&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=11

Organização: School of Data Science, University of Virginia
Moderação: Jess Reia (School of Data Science, University of Virginia - EUA)

Palestrantes: Thallita Lima (Centro de Estudos de Segurança e Cidadania - CESeC - Brasil); María Julia Giorgelli (Defensoría del Pueblo - Argentina); Luã Cruz (Instituto de Defesa do Consumidor - Idec - Brasil)

- O painel reuniu especialistas de três países, dedicados a mapear os impactos de projetos baseados em dados nas cidades, especialmente sobre como interesses privados moldam políticas e serviços públicos. Mesmo em países com regulamentação robusta de dados, como Brasil e Argentina, governos locais enfrentam desafios em equilibrar eficiência e direitos humanos. A implementação de soluções digitais frequentemente ignora opiniões locais e conhecimento comunitário, negligenciando justiça ambiental, igualdade de gênero, proteção de dados e tecnologias de interesse público.

- Foi debatido o diálogo sobre engajamento cívico, burocracia e poder corporativo em cidades latino-americanas. Luã Cruz, do Idec, detalhou casos contestados e a necessidade de proteger direitos em tecnologias invasivas, mencionando o papel da organização "O Panóptico", que discute o viés de discriminação racial nas ferramentas de reconhecimento facial, destacando riscos sociais de seu uso. María Julia Giorgelli, da Defensoría del Pueblo da cidade de Buenos Aires, relatou a suspensão judicial do uso de reconhecimento facial em Buenos Aires e a importância da supervisão rigorosa.

- A audiência participou com perguntas sobre casos semelhantes, destacando desafios. A proteção de dados em cidades requer consideração de infraestrutura e mecanismos de aquisição tecnológica pelos governos. Consultas públicas limitadas não são eficazes para engajamento cívico; uma abordagem multidisciplinar que abrange histórico de direitos, igualdade de gênero e participação social é vital para justiça de dados nas cidades latino-americanas e além.

Biometric data and urban spaces, privacy vs security?

Gravação:
https://www.youtube.com/watchv=PV8mnHErJTg&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=2

Organização: Franco Giandana Gigena (Access Now)
Moderação: Franco Giandana Gigena (Access Now)

Palestrantes: Barbara Simão (InternetLab); Pedro de Perdigão Lana (IODA/ISOC); Raquel Rachid (Lapin)

- A sessão abordou a vigilância urbana baseada em dados biométricos, com foco especial no reconhecimento facial, tendo em vista que o aumento das políticas de vigilância com base em dados biométricos reforça a necessidade de aprofundamento nesse tema. O painel foi uma oportunidade valiosa para fortalecer laços com a sociedade civil e a academia brasileira, marcando um passo significativo na colaboração em questões de vigilância. Os painelistas conseguiram atender às demandas de exposição do CPDP, alcançando uma relação positiva com a plateia. O resultado principal da sessão foi a consolidação dessas conexões, tanto através do envolvimento no espaço designado para perguntas quanto no diálogo contínuo após o término da sessão.

Cine debate: Justiça Social na Era dos Dados

Gravação:
https://www.youtube.com/watchv=m3WkSCSs4H0&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=3

Organização: Associação Data Privacy Brasil de Pesquisa
Moderação: Bruno Bioni (Associação Data Privacy Brasil de Pesquisa)

Palestrantes: Johanna Monagreda, Associação Data Privacy Brasil de Pesquisa; Patrícia Tavares, Defensoria Pública do Estado do Rio de Janeiro; Paola Ricaurte, Instituto Tecnológico y de Estudios Superiores de Monterrey; Juan de Brigard, Fundación Karisma

- O painel, que contou com a moderação de Bruno Bioni, consistiu na exibição do vídeo-documentário Justiça social na era dos dados, documentário produzido pela Associação Data Privacy Brasil e o Coletivo Bodoque, a partir de aprendizados vindos de dois anos de trabalhos em parceria da DPBR e as Defensorias Públicas do Estado de São Paulo e do Rio de Janeiro.
- O curta-metragem apresentou uma visão crítica sobre a proteção de dados pessoais e sua relação com justiça socioeconômica e estimulou o debate em torno de como gênero, raça e classe se apresentam como elementos capazes de determinar a forma diferenciada com que alguns grupos sociais são afetados pelas tecnologias de processamento de dados.
- Johanna Monagreda destacou que o objetivo por trás da produção do documentário foi instigar reflexões sobre a proteção de dados pessoais, não desde uma perspectiva universalizante, mas entendendo que a discussão sobre os riscos precisa ser muito bem situada no contexto brasileiro, especialmente considerando que as desigualdades históricas que atravessam os países latino-americanos colocam desafios muito específicos para considerar, de fato, a proteção de dados pessoais como um instrumento de justiça social.
- Paula Ricaurte argumentou sobre a importância de contextualizar, dentro da geopolítica global, os efeitos dos procedimentos algorítmicos para o Sul global. A palestrante parabenizou o vídeo-documentário no sentido de que permite aproximar os temas da proteção de dados pessoais à cotidianidade da população latino-americana, trazendo temas como a vigilância excessiva de uma forma acessível e em diálogo com o dia-a-dia dos setores populares.
- Juan de Brigard salientou os desafios metodológicos de fazer investigação sobre datificação no contexto latino-americano a partir da experiência da pesquisa com o programa colombiano de transferência de renda “Familias en Acción”. Ainda apontou as dimensões de gênero nos processos de datificação como requisito para o acesso à políticas de assistência social.
- Patrícia Tavares destacou o papel da Defensoria Pública do estado do Rio de Janeiro como órgão de justiça na garantia de direitos da população mais vulnerável.

Enfatizou o duplo papel das DP, como órgão do sistema de justiça na garantia do direito à proteção de dados, e como controlador de uma quantidade vultosa de dados pessoais, inclusive de dados pessoais sensíveis.

Regulação inteligente: o que há na caixa de ferramentas?

Gravação:
https://www.youtube.com/watchv=ayP29m_pLWs&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=23

Organização: Universidade Estadual da Paraíba
Moderação: Cláudio Lucena, Universidade Estadual da Paraíba

Palestrantes: Sizwe Snail (Nelson Mandela University); Clara Langevin (C4IR Brasil); Eduardo Magrani, PhD (Senior Consultant at CCA Law Firm, Affiliate at the Berkman Klein Center of Harvard University)

- Regulação inteligente, ágil, dinâmica e equilibrada em todas as áreas, e particularmente para o cenário de inovação e do ecossistema de convergência digital é um desafio geracional. Instrumentos, recursos e alternativas tradicionais que sempre estiveram disponíveis na caixa de ferramentas regulatórias das várias jurisdições pelo mundo simplesmente já não acomodam muitos dos novos fenômenos e realidades tecnológicas de nosso tempo. Regulamentar, moderar e manter a governança para tecnologias de ponta é um exercício complexo, sobre o qual muito já foi refletido, discutido e debatido. Apesar disso, desdobramentos práticos e alternativas concretas além do repertório convencional ainda precisam e envolvem muita experimentação.
- Esta sessão pretendeu mapear e apresentar algumas dessas novas iniciativas de regulamentação/governança, bem como explorou em quais casos elas foram propostas ou usadas e compartilhar as lições aprendidas nos casos em que foram aplicadas em situações reais.
- Alguns dos principais pontos cobertos foram: *Hard vs Soft* regulation; a importância de regulação e princípios para incentivar o desenvolvimento ético, porém sem criar barreiras desnecessárias para inovação; Avaliações de risco, como Avaliações de Impacto Algorítmicos, que medem os potenciais riscos de uma IA em um contexto específico e a capacidade de uma organização de mitigar tais riscos; Guias como o Guia de Contratações Públicas de IA do C4IR Brasil, em parceria com o Fórum Econômico Mundial, são importantes para nortear boa governança. O Guia reúne diretrizes, recomendações e boas práticas para a contratação de soluções de inteligência artificial (IA) pelo setor público. O objetivo é orientar o servidor público brasileiro. Clara Langevin, da C4IR Brasil buscou adaptar as lições aprendidas no cenário internacional às particularidades da legislação brasileira, com especial atenção ao marco legal que rege as compras públicas, aos atos normativos que

regulam a proteção de dados pessoais, e a maturidade institucional e técnica das entidades públicas brasileiras.

Avaliações de impacto algorítmico: accountability e governança de sistemas de inteligência artificial

Gravação:
https://www.youtube.com/watchv=LXxPW6qG7Vg&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=10

Organização: Prado Vidigal Advogados
Moderação: Carolina Giovanini e Paulo Vidigal, Prado Vidigal Advogados

- A partir das discussões realizadas no âmbito do painel "Avaliações de impacto algorítmico: accountability e governança de sistemas de inteligência artificial", nota-se que é essencial fomentar espaços de discussão multissetorial acerca da regulação da inteligência artificial e, ainda que o debate sobre a regulação esteja sendo travado, há um arcabouço normativo preexistente que, a depender do caso concreto, será aplicável a atividades que envolvam IA.
- No contexto de desenvolvimento de instrumentos de governança para sistemas de IA, a avaliação de impacto algorítmico é uma ferramenta utilizada na identificação de possíveis consequências do desenvolvimento e/ou uso de um sistema de IA para interesses socialmente relevantes. Nesse sentido, as discussões do painel demonstram que tais consequências já não se limitam às questões de privacidade e proteção de dados, mas abrangem outros direitos fundamentais e diversos impactos éticos e sociais.
- As discussões do painel evidenciaram que, assim como ocorrer durante o desenvolvimento das legislações de proteção de dados, a gramática de avaliação de riscos passa a assumir um papel relevante no debate regulatório de IA, de modo que perspectivas iniciais podem ser extraídas dessa estrutura de governança já existente, como no caso da elaboração de relatórios de impacto e adoção de medidas de transparência que efetivamente apresentem critérios de interesse para sujeitos afetados.

Digitalização da educação e tecnologias de vigilância

Gravação:
https://www.youtube.com/watchv=IzgyqtEtfRg&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=17

Organização: Instituto Da Hora; InternetLab
Moderação: Bárbara Simão (InternetLab); Nina Da Hora

Palestrantes: Catarina de Almeida Santos (UNB); Jamila Venturini (Derechos Digitales); Karina Menezes (UFBA); Alexandre Zago Boava (MTST)

- Catarina de Almeida Santos iniciou sua fala questionando o real motivo pelo qual a tecnologia de reconhecimento facial deveria ser implementada nas escolas, lembrando que muitos momentos que ela visa substituir, como o ato de fazer a chamada, são necessários para o desenvolvimento social, e não uma perda de tempo. Ela enfatiza que o que deveria ser feito, é repensar a superlotação das salas de aula. Ela também descreve uma parte do cenário da educação pública brasileira.
- Em seguida, Jamila Venturini descreveu como que a educação está aos poucos, sorrateiramente, sendo privatizada através da tecnologia, citando como exemplo as ferramentas do Google para a Educação. Ela também enfatiza como que câmeras de reconhecimento facial não são uma ferramenta educativa, e sim de vigilância.
- Na segunda fase do painel, Karina Menezes traz uma nova perspectiva sobre a cultura *hacker*, fazendo questionamentos sobre os nossos processos de aprendizagens, alguns já obsoletos, mas que podem ser renovados através do hacker (que significa mudar, redescobrir). Com isso, a professora demonstrou a importância dessa cultura na educação brasileira.
- Por fim, Alexandre Zago Boava, levanta questionamentos sobre a tecnologia, o bem público, a educação e as periferias. Sua fala também levanta pautas sobre racismo e sobre como grandes corporações colocam a tecnologia como inevitável, passando por cima de questões sociais. Em sua conclusão, ele menciona o que está sendo feito para unir a educação com a tecnologia de um modo saudável.

Desafios para o processo de aplicação de penalidades por violação à LGPD no Brasil

Gravação:
https://www.youtube.com/watchv=y2ZyhOq_PmQ&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=5

Organização: Palma Guedes Advogados
Moderação: Tatiana Campos Matos (Palma Guedes Advogados)

Palestrantes: Fabricio Lopes (Coordenador-Geral de Fiscalização da ANPD); Antonio Hiunes (Regulatório das Organizações Globo)

- Os debates ocorridos durante o painel evidenciaram alguns dos principais desafios que vêm sendo enfrentados no que tange à aplicação de sanções por violação à LGPD, destacando-se a preocupação da Coordenadoria-Geral de Fiscalização da ANPD em fixar as penalidades de maneira isonômica e mediante o estabelecimento de diálogos com outras autoridades fiscalizadoras, bem como as expectativas dos agentes de tratamento quanto à promoção de uma regulação responsiva e pautada no diálogo.
- As exposições realizadas pelos painelistas convergiram no sentido de propor reflexões quanto à necessidade de ponderar o nível de gravidade das infrações não só mediante avaliação acerca da existência ou não de dolo pelo agente, mas também através de outros elementos como a pretensão econômica envolvida no tratamento de dados, eventual obstrução do processo fiscalizatório pelo agente e, ainda, a finalidade social da sanção como forma de desincentivar o cometimento de novas infrações.

Identifiable or not? Revisiting data anonymization frameworks in a data-driven world

Gravação:
https://www.youtube.com/watchv=ZBlEbiB1ad4&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=20

Organização: Autoridade Nacional de Proteção de Dados
Moderação: Diego Carvalho Machado, ANPD

Palestrantes: Jonathan Mendoza (Secretary for Data Protection, Mexican Data Protection Authority - INAI); Maria Badillo (Future of Privacy Forum); Laura Galindo Romero (META); Khaled El-Emam (University of Ottawa)

- A proteção de dados e a anonimização na América Latina apresentam desafios e oportunidades no cenário digital em constante evolução. O painel trouxe o debate sobre a eventual necessidade de modificação das técnicas que usamos hoje, considerando que eventualmente precisarão ser apropriadas para gerenciar o risco de identificabilidade no futuro. À medida que a região abraça a transformação digital e a inovação orientada por dados, torna-se imperativo estabelecer estruturas robustas que priorizem os direitos de privacidade dos indivíduos, ao mesmo tempo em que promovem o uso responsável dos dados. A proteção de dados regula o processamento de dados pessoais.
- O painel conclui que a eficácia da anonimização depende, portanto, de uma compreensão sólida do que constitui esses dados. Entende-se que é preciso considerar quem mais pode ser capaz de identificar indivíduos a partir dos dados. Os países da América Latina podem se beneficiar ao adotar uma abordagem abrangente para a proteção de dados, que englobe direitos humanos, medidas legislativas e fiscalização regulatória. É essencial reconhecer o valor dos dados pessoais e estar ciente das transações em que nos envolvemos ao acessar serviços online gratuitos. Assumir o controle de nossa privacidade e compreender as compensações pode nos capacitar a tomar decisões mais informadas no mundo digital.

O Open Health do Brasil encontra o European Health Data Space: desafios de portabilidade, dados abertos e reaproveitamento de dados de saúde

Gravação:
https://www.youtube.com/watchv=fEdVSfWBt2g&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=12

Organização: Nicolo Zingales (MyData Brasil)
Moderação: Nicolo Zingales (MyData Brasil)

Palestrantes: Tjasa Petrocnik; Diogo Richter (CTS-FGV); Camila Leite (IDEC); Jenifer Rodriguez (Max Planck Institute for Competition and Innovation)

- Os participantes apresentaram e discutiram questões relacionadas ao acesso, análise e compartilhamento de dados de saúde; a origem de iniciativas voltadas para abordar esses problemas, geralmente referidas como "Saúde Aberta"; os desafios legais, regulatórios, tecnológicos, infraestruturais e de governança associados à implementação da Saúde Aberta no Brasil e ao Espaço Europeu de Dados de Saúde na União Europeia.
- Foi observado que, tanto no Brasil quanto na União Europeia, a Saúde Aberta precisa cumprir requisitos específicos e garantias fornecidas pelas regulamentações de proteção de dados pessoais, como a LGPD (Lei Geral de Proteção de Dados) e o GDPR (Regulamento Geral de Proteção de Dados), para permitir a portabilidade de dados de acordo com os propósitos e expectativas pretendidos pelos usuários do sistema de saúde.
- Ficou demonstrado que, para o desenvolvimento adequado de um ecossistema de dados de saúde, é necessário identificar os atores relevantes dentro da estrutura existente, desenvolver uma infraestrutura tecnológica que considere o modelo de governança adotado para esse ecossistema e centralizar a criação de uma infraestrutura de Saúde Aberta para permitir o uso de dados pelos pacientes, não apenas - ou especialmente - pelos prestadores de serviços de saúde.
- Também foi argumentado que, no contexto brasileiro, a Saúde Aberta carece de discussão política e social adequada, uma vez que os promotores do governo de tais iniciativas não incluíram todos os atores envolvidos no sistema de saúde no debate. Por fim, foram discutidas as convergências e divergências entre as iniciativas de Saúde Aberta e Open Banking. Embora compartilhem nomes semelhantes, as características dos sistemas que eles abrangem respectivamente - sistema de saúde e

sistema financeiro - são distintas (por exemplo, sistema público vs. sistema privado; concentração vs. fragmentação de prestadores de serviços; regulamentação centralizada em nível federal vs. regulamentação distribuída em todos os níveis governamentais). Devido a isso, as soluções encontradas para a implementação do Open Banking, embora potencialmente sirvam como "lições aprendidas" para a Saúde Aberta, não são necessariamente compatíveis com esta última.

Developing New Tools to Make AI More Explainable

Gravação:
https://www.youtube.com/watchv=3wuST2OMowc&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=16

Organização: Meta
Moderação: Polina Zvyagina (Meta)

Palestrantes: Rumman Chowdhury (AI Fellow at the Berkman Klein Center); Diogo Cortiz (PUC SP / CEWEB); Iga Kozlowska (Meta); Jonathan Mendoza (INAI)

- Os sistemas de IA representam um salto significativo nas capacidades de processamento de informações, utilizando modelos e algoritmos que podem aprender e realizar tarefas cognitivas complexas. Esses sistemas se tornaram um intermediário crucial entre humanos e computadores, dando origem a importantes considerações éticas. A tomada de decisões em diversos aspectos da vida cotidiana, como no local de trabalho, interações sociais, cuidados de saúde e educação, agora é impactada pela tecnologia de IA.
- À medida que a tecnologia avança e nossa dependência de dispositivos digitais aumenta, o volume de dados pessoais coletados e processados cresceu exponencialmente. Para abordar preocupações com a privacidade, tecnologias de aprimoramento de privacidade (PETs) foram desenvolvidas, garantindo segurança e confidencialidade dos dados enquanto permitem o compartilhamento responsável de dados. Embora os avanços tecnológicos ofereçam inúmeros benefícios, eles também apresentam desafios significativos para a privacidade e a segurança de dados.
- Na América Latina, medidas têm sido adotadas para abordar questões relacionadas à IA. No entanto, desafios éticos decorrentes de algoritmos de IA que reforçam preconceitos existentes e perpetuam comportamentos discriminatórios exigem cooperação internacional.
- As recomendações da UNESCO defendem frameworks regulatórios que incentivem a adesão a padrões éticos, promovendo direitos humanos, democracia e ética. Por meio de ferramentas de avaliação de impacto, o objetivo é avaliar e mitigar os riscos apresentados pelas novas tecnologias, garantindo seu impacto positivo nas sociedades e a manutenção do Estado de Direito. Enfatizar a transparência e a explicabilidade nos sistemas de IA é crucial para capacitar os usuários com uma compreensão clara das capacidades e limitações da tecnologia.

- Ao colaborar com organizações internacionais, setores privados, sociedade civil e academia, o México se esforça para estabelecer frameworks pragmáticos, inclusivos e operacionais de governança de IA.

Exploring Vulnerabilities and Asymmetries in Latin America: Implications for Data Protection Rights of Vulnerable People

Gravação:
https://www.youtube.com/watchv=vTfv_ZivZY&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=19

Organização: Cedis/IDP & Data Privacy Brasil
Moderação: Diego Carvalho Machado (UFV/CEDIS-IDP)

Palestrantes: Johanna Monagreda (Data Privacy Brasil); Valeria Milanes (ADC); Ramon Costa (NIC.br e PUC-Rio); Paola Ricaurte (Escuela de Humanidades y Educación, del Tecnológico de Monterrey)

- Valeria Milanes compartilhou a oportunidade de melhorar as ferramentas de proteção de dados - principalmente para grupos em situação vulnerável - que a Argentina tem, dada a proposta de lei de proteção de dados apresentada ao Congresso no final de junho, como: o princípio da "preeminência", no caso de dúvida, a interpretação mais favorável ao titular dos dados deve prevalecer; e o reconhecimento da "ação coletiva" para o habeas data, que pode ser proposta como uma representação coletiva pela Agência de Proteção de Dados, o Ouvidor-Geral ou associações ou organizações com interesse legítimo.
- Paola Ricaurte introduziu o conceito de vulnerabilidade e destacou que na América Latina existem maiores desafios em proteger pessoas vulneráveis devido a assimetrias sociais e desigualdades. Essas condições em um mundo de dados aumentam as vulnerabilidades e a discriminação ilegal, especialmente em grupos como imigrantes, povos indígenas e crianças.
- Johanna Monagreda destacou a história de dominação sobre certos grupos sociais, especialmente comunidades negras, e como isso impacta o desenvolvimento de tecnologias, como sistemas de vigilância para segurança pública. Portanto, é importante questionar a suposta neutralidade da economia orientada por dados, incluindo a coleta de dados e outros meios de processamento de dados.
- Ramon Costa abordou a proteção de dados pessoais no Brasil. Ele concentrou-se em dados pessoais sensíveis e explorou como essa categoria especial de dados está relacionada à noção de vulnerabilidade.

The collective approach to privacy - anonymity sets, mixnets and reversing the surveillance business incentive

Gravação:
https://www.youtube.com/watchv=i4lKhhSAaOU&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=24

Organização: Nymtech
Moderação: Daniel Vazquez, Nymtech

Palestrantes: Daniel Vazquez (Nymtech); Jamila Venturini (Derechos Digitales); Rafael Zanatta (Data Privacy Brasil)

- As discussões no painel começaram com Daniel apresentando a solução da Nym como um todo e discutindo como podemos usar a tecnologia para combater a vigilância em massa de empresas e governos. Ele incentivou uma abordagem proativa para o problema, onde imporíamos a privacidade em vez de pedir por ela e esperar. Após Daniel estabelecer o cenário com as discussões iniciais sobre a Nym, os outros dois participantes apresentaram suas opiniões sobre os problemas atuais de vigilância e privacidade.
- Rafael Bonifaz falou sobre a cultura cyberpunk e como a web poderia ser um lugar onde podemos construir um novo paradigma que se afaste do modelo atual de coleta massiva de dados e destacou a importância dos direitos digitais e como eles não têm sido respeitados.
- Rafael Zanatta falou sobre a situação atual da luta contra a vigilância, mencionando como não podemos esquecer pessoas como Snowden e Assange, que ainda enfrentam consequências por expor irregularidades e lutar contra o modelo atual de extração de dados, destacando também a importância de criar regulamentações eficazes que impeçam esse modelo de prosperar e crescer.
- Em seguida, o público teve a oportunidade de fazer perguntas e adicionar comentários, abordando desde bitcoin, leis, ações possíveis a serem tomadas até movimentos atuais que combatem o modelo de negócios e cultura de vigilância em que vivemos.

Comparative Approaches to Facial Recognition Regulation

Gravação:
https://www.youtube.com/watchv=eTG1ua1_ANc&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=4

Organização: Camila Leite Contri (Idec - Instituto Brasileiro de Defesa do Consumidor)
Moderação: Walter B. Gaspar (CTS-FGV Direito Rio)

Palestrantes: Camila Leite Contri (Idec - Instituto Brasileiro de Defesa do Consumidor); Andrew Miller (Yale Law School); Maria Julia Giorgelli (Defensoría del Pueblo de la Ciudad de Buenos Aires)

- O painel abordou o aumento da tecnologia de reconhecimento facial em vários países da região e do mundo e discutiu como melhorar, projetar e aplicar essas proteções de maneira complexa.
- Cada um dos palestrantes explicou a situação em seu próprio país (Argentina, Brasil e EUA), permitindo assim a comparação entre sistemas jurídicos, e incluiu representantes com experiência relevante nos setores governamentais, da sociedade civil, acadêmico e de litígios privados.
- Alguns dos tópicos discutidos foram: o escopo das proteções relevante; os objetivos que essas proteções buscam alcançar; mecanismos específicos de aplicação (ações individuais vs. ações coletivas/representativas, aplicação privada vs. pública, direito à privacidade vs. direito do consumidor, etc.); o papel da sociedade civil e/ou do setor privado na busca ou estímulo a ações de aplicação; os recursos disponíveis quando violações são descobertas; e autoridade sobreposta entre agências governamentais, entre outros.

Data Protection and Generative AI: current legal obligations and what should we expect from the upcoming AI Regulation initiatives worldwide

Gravação:
https://www.youtube.com/watchv=3tMZ6p53mmU&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=13

Organização: Cedis/IDP; Access Now
Moderação: Mônica Fujimoto (CEDIS/IDP)

Palestrantes: Franco Giandana Gigena (Access Now); Dora Kaufman (PUC/SP); José Renato Laranjeiras (Lapin); Paula Guedes (Data Privacy Brasil); Luca Belli (CTS FGV)

- A Access Now e o CEDIS/IDP organizaram de maneira conjunta uma sessão sobre regulamentação de Inteligência Artificial, focando particularmente na IA generativa. O objetivo central do painel foi possibilitar o debate entre especialistas com bagagem multidisciplinar sobre a regulamentação de tecnologias de Inteligência Artificial Generativa, considerando as suas especificidades, riscos, benefícios e discutir possíveis contribuições para o desenvolvimento do marco regulatório brasileiro. Nesse sentido, o painel foi moderado por Mônica Fujimoto (CEDIS-IDP) e contou com a participação dos painelistas Luca Belli (CTS FGV), Dora Kaufman (PUC/SP), José Renato Laranjeiras (Lapin), Franco Giandana Gigena (Access Now) e Paula Guedes (Data Privacy Brasil).
- Inicialmente Luca Belli discutiu os principais conceitos envolvendo a IA Generativa e os principais motivos pelos quais ela se diferencia de outras tecnologias até então desenvolvidas, citando o exemplo de seu peticionamento perante a ANPD sobre o uso de dados pessoais por modelos de inteligência artificial de grande escala, como o Chat GPT. Dora Kaufman apresentou a relação desta tecnologia com a proteção de dados pessoais e como boas práticas podem ser adotadas, a exemplo da adoção de padrões (standards) que podem reduzir os custos de compliance, destacando que a regulação exige a atuação de diversos setores.
- Em seguida, para uma perspectiva comparada, José Renato Laranjeiras apresentou o endereçamento do assunto na União Europeia (“AI Act”, aprovado em junho de 2023 pelo Parlamento Europeu) e como tal debate poderia ou não influenciar as discussões brasileiras. Sob a perspectiva da América Latina, Franco Giandana Gigena discutiu iniciativas regulatórias em alguns países, até então mais centralizadas no uso de IA pelo poder público, e apresentou as propostas legislativas de países sobre IA como Peru, Chile e Costa Rica. Por fim, a respeito da perspectiva brasileira, Paula Guedes compartilhou suas considerações sobre o Projeto de Lei 2.338/2023, resultado do trabalho da CJSUBIA, que, ainda que não apresente uma menção direta ao termo “Inteligência Artificial Generativa”, apresenta em seu art. 30 elementos que

podem auxiliar na regulação responsiva, como a possibilidade de elaboração de códigos de boas práticas e de governança pelos agentes de IA.

Exploring the Evolving World of Cross Border Transfers: Contracts, Adequacy, Certifications and More in 2023 and Beyond

Gravação:
https://www.youtube.com/watchv=Fqb5RE2Whig&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=18

Organização: The Future of Privacy Forum
Moderação: Lee Matheson, The Future of Privacy Forum

Palestrantes: Lucas Borges de Carvalho (ANPD); Marcela Mattiuzzo (VMCA Advogados); Carolina Rossini (Co-Founder and Director for Policy and Research, The Datasphere); Sam Schofield (Sr. Policy Advisor in the Office of Digital Services Industries (ODSI) at the U.S. Department of Commerce)

- Marcela iniciou o painel discutindo as transferências transfronteiriças no contexto de sua experiência como advogada na área de privacidade. Ela enfatizou em particular que, em toda a região da América Latina, a incerteza em relação às obrigações relacionadas às transferências de dados e a crescente multiplicidade de regras eram fatores significativos para os custos de conformidade.
- Lucas Borges discutiu a agenda atual da ANPD e o progresso esperado em relação às transferências transfronteiriças e à aplicação esperada da LGPD, compartilhando com o público algumas informações sobre o cronograma das próximas publicações da ANPD; incluindo a expectativa de vermos o rascunho da regulamentação de transferência de dados da ANPD antes do final do ano.
- Sam Schofield fez uma breve apresentação sobre o novo Sistema Global de Regras de Privacidade Transfronteiriça, atualmente promovido pelos Estados Unidos, delineando a estrutura do Sistema e fornecendo algumas informações sobre seu passado como uma ferramenta de transferência de dados específica da APEC.
- Por fim, Carolina Rossini discutiu o papel dos "sandboxes" regulatórios no avanço da política de proteção de dados, especialmente no que diz respeito à IA e ao processamento algorítmico de dados pessoais. Carolina também observou os próximos papéis do Brasil na presidência das organizações BRICS e G20. Os temas gerais incluíram a dificuldade de convergência entre sistemas globais de proteção de dados que estão proliferando substancialmente e o papel dos contratos em preencher as lacunas entre leis nacionais de proteção de dados substancialmente diferentes.

Os riscos dos dados – os desafios da conformidade com a sobreposição de regulações baseadas em risco

Gravação:
https://www.youtube.com/watchv=tVlAgzodbFE&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=22

Organização: Autoridade Nacional de Proteção de Dados
Moderação: Thiago Guimarães Moraes, ANPD

Palestrantes: Bojana Bellami (CIPL); Lia Hernandez (IPANDETEC); Beatriz Kira (UCL); Rodrigo Santana dos Santos (ANPD)

- Durante nossa intervenção, descrevemos os objetivos gerais da associação IPANDETEC, que está presente na América Central e cujos esforços estão principalmente no âmbito da defesa, disseminação e regulamentação dos direitos humanos em ambientes digitais. Parte das abordagens que desenvolvemos em nossos estudos e análises da região demonstram as deficiências estruturais e as oportunidades de melhoria na infraestrutura tecnológica de cada um dos Estados.
- Em nossa intervenção, enfatizamos que um grande problema que afeta todos os países da região é o risco de corrupção, e que sua manifestação muitas vezes impede que o aparato judicial atue para defender a vítima. Também comentamos sobre disciplinas coexistentes, como a proteção de dados pessoais e a devida diligência para a prevenção de lavagem de dinheiro e outros crimes, bem como a vigilância por vídeo do cidadão e o direito à imagem.
- Nesse contexto, mencionamos alguns efeitos adversos que surgem dessa coexistência, no entanto, consideramos que existem mecanismos para atingir os objetivos e que, em grande medida, dependemos da colaboração de todas as partes interessadas e da divulgação para a sociedade em geral.

AI and Automated Personal Data Processing in the BRICS Countries

Gravação:
https://www.youtube.com/watchv=hDtwhL9R3nM&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf

Organização: CyberBRICS
Moderação: Luca Belli, CyberBRICS

Palestrantes: Lygia Calvino (Privacy Officer, Huawei Technologies, Latin American Department) ;Ekaterina Martynova (Higher School of Economic, Moscow); Smriti Parsheera (CyberBRICS); Wei Wang (Hong Kong University); Sizwe Snail (Snail Attoneys);

This session featured a diverse array of stakeholder opinions, presentations and case studies analysing the implications of AI governance and automated data processing in the BRICS countries.

- Ms Lygia Calvino presented Huawei's view on the characteristics of AI and its healthy development, which relies on sound governance of AI, cybersecurity, and privacy protection. Calvino stressed that AI activities involves four key roles, namely, consumers/customers, deployers, solution providers, and data collectors. The overall AI governance objectives are mainly considered from seven aspects: System security and controllability, Transparency and traceability, Privacy Protection, Fairness, Data management, Competence and Deployment objective assurance. Therefore, Huawei understands the importance of defining the responsibilities based on the concept of AI shared responsibility. Calvino stressed that Huawei channels its expertise into bolstering AI security and privacy protection, and provides innovative ICT infrastructure and smart devices to global carriers, enterprises, governments, and individual consumers, effectively promoting digital transformation and creating enriched value for society. Huawei also understands that it is not only vital to the healthy development of human society in the digital era, but also Huawei's incumbent responsibility to actively support the establishment, implementation, and improvement of security and privacy standards in the digital era, as well as help countries develop and establish their own digital era and processes.
- Ms Ekaterina Martynova, CyberBRICS Visiting Researcher from the Higher School of Economic, Moscow, presented an overview of the National Strategy on the development of AI in Russia. She highlighted the key principles for regulating relations using AI with a focus on technological sovereignty and a risk-based, interdisciplinary approach to regulation. Based on the case-study of an experimental introduction of AI in the healthcare system of Moscow she described how the requirements of transparency, accountability and anonymization of personal data are met when implementing innovative computer vision technologies for medical image analysis and subsequent applicability in the Moscow hospitals.
- Ms Smriti Parsheera, CyberBRICS Fellow, provided an outline of India's approach to AI and data governance. She explained that India is currently not looking at a regulatory framework

on AI and the emphasis is more on encouraging innovation and collaborations. The country has, however, articulated a national AI strategy and principles for responsible AI for All. This was followed by a deep dive into one particular application - the DigiYatra system for automation of airport procedures using facial processing. She described the design and components of this system and highlighted key challenges of such projects.

- Mr Wei Wang, CyberBRICS Fellow from Hong Kong University, showcased the recent updates in data and AI governance in China, with a particular focus on the emergence of generative AI. He argued that the country has adopted a hybrid sectoral model, encouraging innovation in AI within government-set economic development plans. The results are evident in indicators that place the Chinese at the top in research and academic citations. On the other hand, ethics in the use and development of AI is also promoted by the government through numerous dedicated committees. After this overview, the researcher briefly touched on the existing legislation regarding data governance, highlighting its key provisions. He also showed us that, unlike most countries, AI development in China is not controlled by a small number of companies but is carried out by mostly medium and large enterprises. He concluded by commenting on a draft law for AI, which was submitted for assessment by Chinese lawmakers.
- Professor Sizwe Snail addressed the South African context, emphasizing the importance of using the constitution as a reference point in discussions about AI. He highlighted the fundamental rights protected by it. Despite the absence of specific legislation on AI, existing regulations, such as the Electronic Communications and Transactions Act (ECT Act) and the Cybercrimes Act, are being invoked in legal decisions related to automated decisions. After these considerations, the researcher presented two specific cases in South Africa regarding the misuse of AI in legal proceeding at the South African level.

Suggested readings: Luca Belli, Danilo Doneda. Data protection in the BRICS countries: legal interoperability through innovative practices and convergence. International Data Privacy Law, Volume 13, Issue 1, February 2023. https://doi.org/10.1093/idpl/ipac019

Data Transfers and eCommerce: Towards International Cooperation

Gravação:
https://www.youtube.com/watchv=V5YmLn0DbJE&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=14

Organização: Diplo Foundation & Women Inside Trade
Moderação: Dolores Dozo, Key Latam expert, EU funded Project on Enhanced Data Protection and Data Flows; Nicolo Zingales, CTS-FGV

Palestrantes: Felipe Palhares (Sócio do BMA Advogados); Marilia Maciel (Diplo Foundation & Women Inside Trade); Jonathan Mendoza, (Secretary for Data Protection, Mexican Data Protection Authority - INAI); Carolina Rossini (Co-Founder and Director for Policy and Research, Datasphere)

- Dados pessoais são uma questão global, nesse sentido, é necessário estabelecer um padrão internacional, que pode ser alcançado por meio da interoperabilidade. No entanto, as transferências internacionais de dados enfrentam vários desafios, considerando sua importância na economia digital, elas se tornam práticas essenciais, devendo cumprir padrões de qualidade e segurança para os usuários. Isso considerando que, em alguns casos, sua implementação é complexa devido às diferentes regulamentações em cada país e à incessante inovação tecnológica que oferece novas formas de comercialização de produtos e serviços a cada dia.
- Nesse sentido, alguns dos desafios incluem garantir a proteção e privacidade dos dados durante as transferências internacionais, a jurisdição e os quadros regulatórios, a segurança dos dados, o consentimento informado, as transferências para países com níveis inadequados de proteção, bem como a transparência e a responsabilidade.
- Para enfrentar esses desafios, foram estabelecidos quadros legais e mecanismos de autorregulação, como acordos de transferência de dados e padrões de segurança, para garantir uma proteção adequada dos dados e o respeito aos direitos de privacidade nas transferências internacionais de dados.
- Uma prática que deve ser incentivada é a adoção de esquemas de autorregulação vinculativa, bem como a adoção de instrumentos jurídicos específicos, como cláusulas modelo ou regras corporativas vinculativas.
- Portanto, na América Latina, é necessário desenvolver um quadro regional adequado para o reconhecimento da adequação das jurisdições locais, a fim de permitir o fluxo livre de dados dentro de um quadro protetor dos direitos de proteção de dados pessoais.

La regulación de sistemas nacionales de identidad: propuestas de cooperación regional

Gravação:
https://www.youtube.com/watchv=__XDnSzgm60&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=21

Organização: Fundación Karisma
Moderação: Hannah Draper, Collaborative cash distribution (CCD)

Palestrantes: Marianne Díaz Hernández (Access Now); Eduardo Carrillo (TEDIC); Marina Meira (Asociación Data Privacy Brasil de Investigación); Juan de Brigard (Fundación Karisma)

- No painel, foram apresentadas as situações atuais dos sistemas de identidade no Brasil, Paraguai e Colômbia, oferecendo também uma perspectiva regional. Graças às diversas intervenções, foi possível identificar semelhanças entre os sistemas da região.
- Discutiu-se os diversos usos dados aos sistemas de identidade digital na região, assim como as narrativas de soluções tecnológicas que sustentam seu avanço em várias áreas, como processos eleitorais e acesso a serviços do Estado, entre outros.
- Também foi abordado o papel das empresas privadas provedoras de tecnologia, frequentemente as mesmas empresas do Norte global que operam em toda a região. Além disso, a discussão permitiu identificar estratégias de influência e abordagens chave de ação para as organizações da sociedade civil (OSCs).
- Nesse sentido, enfatizou-se a importância de mostrar os limites da digitalização como solução absoluta, ou seja, a relevância de apresentar contra narrativas que questionem o avanço irrestrito da tecnologia sem avaliações prévias dos direitos humanos.
- Abordou-se os limites da abordagem legalista em relação à proteção de dados pessoais e a tensão entre a necessidade de garantir a identidade legal, por um lado, e a necessidade de fazê-lo com plenas garantias de acesso e privacidade, por outro.
- Por fim, três grandes questões profundamente interconectadas e associadas aos sistemas digitalizados de identidade em nossa região foram focadas: o monopólio de determinados atores privados sobre a tecnologia, a perda de soberania nacional decorrente da dependência de tecnologias estrangeiras para a identificação nacional, e as práticas corruptas em torno da contratação de serviços e infraestruturas de identidade digital.

Neuroderechos: una discusión impostergable sobre derechos humanos y protección de datos

Gravação:
https://www.youtube.com/watchv=uhPEL-DgGaU&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=6

Organização: Instituto de Referência em Internet e Sociedade (IRIS)
Moderação: Juliana Roman, IRIS

Palestrantes: Rafaela Ferreira Gonçalves da Silva (Universidade Federal da Bahia - UFBA); Moisés Sánchez (Fundación Kamanau); Natalia Monti (Fundación Kamanau); Bárbara Muracciole (Universidad de la República); Rafael Yuste (Columbia University / NeuroRights Foundation)

- O painel alcançou o objetivo de posicionar o tema na agenda da academia, empresas, organizações da sociedade civil e Estados. A apresentação ofereceu uma visão geral sobre a proteção jurídica da atividade neural, incluindo casos práticos de experiências neurocientíficas atuais e produtos de tecnologias imersivas que utilizam neurodados. Além disso, apresentou um panorama dos importantes movimentos de construção normativa na área, como é o caso da proposta de reforma constitucional brasileira n.º 522/22, que visa conferir proteção especial aos dados neuronais.
- Por outro lado, em resposta ao apelo dos neurocientistas, o painel trouxe discussões que demonstraram a necessidade de atenção aos aspectos normativos necessários para a proteção dos direitos humanos afetados pelas neurotecnologias, não apenas em uma perspectiva futurista, mas também na atualidade.
- Nesse sentido, os participantes destacaram que o painel os enriqueceu com elementos concretos, como os Princípios Interamericanos no âmbito da OEA. Além disso, reconheceram as vantagens do uso das neurotecnologias, como no tratamento de pessoas neurodivergentes, desde que sejam desenvolvidas e utilizadas de maneira ética. Dessa forma, do ponto de vista jurídico, seria possível oferecer uma primeira proteção enquanto se desenvolvem discussões mais amplas sobre a necessidade de reconhecimento dos neurodireitos e a implementação de instrumentos internacionais de Direitos Humanos adicionais aos já existentes.
- No âmbito desse debate, despertou interesse especial a proposta de considerar os neurodados como sensíveis, conforme a proposta desses princípios. Isso envolve reformar as leis existentes ou incluí-los nas novas normas a serem promulgadas, a fim de oferecer uma resposta imediata diante da iminente utilização desse tipo de informação por empresas e Estados.
- Além disso, a audiência refletiu sobre a pertinência de incluir ou não explicitamente o neurodado, concluindo que tal inclusão seria necessária se considerado "sensível".

No entanto, sugeriu-se o reconhecimento explícito em todos os casos, a fim de evitar interpretações que o excluam da categoria de "dado pessoal".

- Outra preocupação relacionada à regulamentação por meio das normas de proteção de dados diz respeito à possível afetação do princípio de neutralidade tecnológica. A dúvida foi esclarecida, uma vez que a proposta do painel se referia a regulamentar o neurodado como pessoal e sensível, sem mencionar as (neuro)tecnologias envolvidas em sua coleta, portanto a neutralidade não seria afetada.
- O desenvolvimento do painel foi muito inovador para alguns dos participantes. Alguns notaram que o trabalho que vinha sendo realizado sobre o tema era desconhecido por muitos acadêmicos da área de dados pessoais e que achavam a discussão extremamente interessante e atrativa para ser incluída em outras discussões e seminários a nível local, regional e global.

Desafios da Transparência na Inteligência Artificial: Garantindo Justiça e Responsabilidade

Gravação:
https://www.youtube.com/watch?v=aFw3SOu9Qe4&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=15

Organização: Instituto da Hora
Moderação: Nina da Hora, Instituto da Hora

Palestrantes: Bianca Kremer (IDP); Pablo Nunes (Panóptico / CESEC)

- O painel reuniu especialistas e profissionais para debater questões cruciais relacionadas à utilização adequada e justa de sistemas tecnológicos, bem como as implicações jurídicas e sociais associadas. O painel reuniu especialistas e profissionais para debater questões cruciais relacionadas à utilização adequada e justa de sistemas tecnológicos, bem como as implicações jurídicas e sociais associadas.
- Nina da Hora, a anfitriã do painel, destacou que a proposta central era explorar a interligação entre justiça e tecnologia, abrangendo tanto aspectos de justiça racial quanto social. O escopo ia além do mero marco regulatório da Inteligência Artificial (IA), buscando compreender a dinâmica entre Estado, empresas e o terceiro setor na interlocução sobre o tema.
- A primeira pergunta abordou como garantir a responsabilização dos profissionais envolvidos no desenvolvimento de tecnologias, especialmente em casos de danos resultantes do uso inadequado ou injusto desses sistemas.
- Bianca ofereceu uma perspectiva do direito civil, ressaltando que a falta de um regime jurídico unificado no campo tecnológico é resultado de disputas políticas. Ela destacou que as empresas de tecnologia muitas vezes favorecem pontos de vista que beneficiam seus interesses econômicos, prejudicando a resposta a danos ocorridos.
- Pablo, por sua vez, abordou o tema da responsabilização a partir da ótica da segurança pública, observando os desafios de impor responsabilidade em um contexto de opacidade e resistência por parte das forças de segurança estatal.
- A segunda pergunta concentrou-se na Lei Geral de Proteção de Dados (LGPD) e como ela impacta a responsabilização e a melhoria contínua dos serviços tecnológicos. Nina indagou sobre a viabilidade de manter os dados dos usuários por até 10 anos sem prejudicar a inovação.
- Bianca enfatizou a falta de debate sobre desenvolvimento econômico e tecnológico na regulação, destacando a dependência tecnológica do Brasil em relação a tecnologias estrangeiras. Ela defendeu a necessidade de reforçar incentivos estatais para a produção de tecnologia nacional. Pablo introduziu a dimensão geopolítica, mencionando exemplos como a disputa entre empresas chinesas e americanas pelo mercado brasileiro.

- A discussão trouxe à tona preocupações relacionadas à representatividade nas avaliações de impacto e na ausência de órgãos de representação dos trabalhadores no diálogo sobre tecnologia. A falta de trabalhadores qualificados na área tecnológica também foi mencionada como um desafio. Em suma, o painel ofereceu uma visão abrangente das complexas questões de justiça, responsabilização e tecnologia, destacando a necessidade de abordagens multidisciplinares e colaborativas para enfrentar esses desafios em evolução.

Responsabilidade Civil na LGPD: dados empíricos e ensaios críticos

Gravação:
https://www.youtube.com/watchv=9xMUAYWv1kA&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=26

Organização: Arquitetura Educacional & Macher Tecnologia
Moderação: Nicolo Zingales (FGV Direito Rio)

Palestrantes: Erica Bakonyi (FGV Direito Rio, Arquitetura Educacional e Macher Tecnologia); Bruno Bioni (Data Privacy Brasil); Caitlin Mulholland (Direito PUC Rio); Daniel Dias (FGV Direito Rio); Rodrigo Pinho Gomes (Pinho Gomes Advogados)

- A partir da análise de dados empíricos relentes às decisões judiciais e a responsabilidade civil face à LGPD, os painelistas debateram sobre os desafios da matéria. Buscou-se superar a dualidade das teorias objetiva e subjetiva da responsabilidade civil, no intuito de aprofundar os ensaios críticos. Exploraram-se conceitos tradicionais do Direito Civil e possíveis soluções para as métricas a serem utilizadas na dosimetria das indenizações, bem como a possibilidade de se adotar a teoria do dano presumido (in re ipsa) como, por exemplo, perda do controle dos dados pessoais pelo seu respectivo titular.

Telemarketing sem consentimento: um desafio à proteção de dados na América Latina

Gravação:
https://www.youtube.com/watchv=TMr8OGID2U&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=25

Organização: Instituto Brasileiro de Defesa do Consumidor
Moderação: Luã Cruz (IDEC)

Palestrantes: Camila Leite (Idec - Brasil); Rocío Romero (Salud con Lupa - Peru)

- O painel focou em trazer problemas e soluções para o telemarketing abusivo. A jornalista Rocio Romero trouxe uma análise de caso da investigação que apontou o assédio moral sofrido pela população peruana com ofertas de telemarketing para adesão a planos de saúde - como ligações com ameaças psicológicas para ter um plano de saúde, se aproveitando do medo da população para convencê-la a ter o plano. Nesse caso, assim como em outros países, as ligações foram feitas a pessoas com quem essas empresas não tinham relação prévia e de quem não se sabem como se conseguiu as bases de dados.
- A ilegalidade no acesso a base de dados de telefones e nomes de pessoas é um dos pontos que também foi analisado na nota técnica publicada pelo Idec - Instituto Brasileiro de Defesa do Consumidor, exposta pela palestrante Camila Leite, quem fez uma abordagem levantando os problemas do telemarketing abusivo para fins de direitos de consumidores, para a regulação de telecomunicações e para a proteção de dados.
- A nota técnica, também produzida pelo moderador Luã Cruz, foi também comentada por Ramon Costa. No momento das dúvidas, um debate relevante foi a discussão se poderia ser utilizada a base legal do legítimo interesse para a realização dessas ligações.

Unveiling the Duality of Digital ID in Latin America: Empowering or Burdening Individuals?

Gravação:
https://www.youtube.com/watchv=eZKgNJqsZMM&list=PLspVbtJ_9_Hq1VbsRfwp7IQ4sBiG0h9yf&index=7

Organização: CPDP Brussels
Moderação: Andrés Chomczyk Penedo, CPDP/Vrije Universiteit Brussel, Belgium

Palestrantes: Marina Meira (Data Privacy Brazil - Brasil); Marcos Lopez Allende (Interamerican Development Bank - International); Javiera Sepúlveda (Bitlaw - Chile); Sophie Stalla-Bourdillon (University of Southampton / Immuta / Brussels Privacy Hub - UK); Andrés Chomczyk Penedo (CPDP/Vrije Universiteit Brussels Belgium); Pablo Trigo Kramcsak (CPDP / Vrije Universiteit Brussel - Belgium)

- Os sistemas de Identificação Digital desempenham um papel fundamental no impulso da Indústria 4.0, no Governo Eletrônico e na inclusão digital em setores como saúde, finanças, comércio eletrônico, prestação de serviços públicos e outras áreas orientadas por dados. A integração da Identificação Digital com a proteção de dados apresenta muitos desafios. Questões como processamento legal, minimização de dados, limitação de propósito e proteção de dados por design e padrão fazem parte dessas preocupações.
- Esta sessão abordou o processamento de dados pessoais em iniciativas de Identificação Digital na América Latina (atuais e futuras), especialmente aquelas baseadas em blockchain, considerando o impacto das novas leis de proteção de dados inspiradas no GDPR.
- O objetivo do painel era promover uma compreensão mais profunda da dimensão de proteção de dados na governança da Identificação Digital e das carteiras digitais.
- Principais questões discutidas: - Como funcionam e operam os sistemas de Identificação Digital e quais riscos de privacidade eles envolvem? - Como as organizações e formuladores de políticas podem equilibrar o fomento à inovação digital e a defesa dos direitos dos titulares de dados no âmbito da Identidade Digital?
- Marcos Lopez Allende forneceu uma visão geral do presente (Web 2.0) e do futuro (Web 3.0) das carteiras digitais, o que foi muito útil como contexto para a discussão.
- Sophie Stalla-Bourdillon referiu-se à abordagem e à perspectiva da UE sobre identidade digital e proteção de dados, mantendo especialmente em mente o proposto framework eIDAS 2.
- Javiera Sepúlveda abordou a Identificação Digital a partir da perspectiva do setor privado, abrangendo os principais desafios que esses sistemas (centralizados e

descentralizados) representam para a indústria, usando o setor de serviços financeiros e as políticas de open banking como exemplo.

- Marina Meira mencionou algumas preocupações da perspectiva da sociedade civil relacionadas às identidades digitais, apresentando uma abordagem do sul global, com foco em se as pessoas têm as competências digitais para interagir efetivamente com essas novas ferramentas.
- Andrés Chomczyk Penedo mencionou algumas considerações legais e regulatórias relacionadas às identidades digitais e carteiras digitais baseadas em blockchain, e como a confiança nas relações peer-to-peer pode influenciar as decisões de compartilhamento de dados das pessoas.
- A sessão de Perguntas e Respostas englobou "Modelos de Auto-Identificação Centralizados vs. Descentralizados". Ambos os modelos oferecem vantagens e desvantagens; seu sucesso deve depender se eles realmente promovem uma melhor proteção para os indivíduos. Abordar as principais preocupações de proteção de dados e privacidade associadas a cada modelo foi o foco principal desta parte do painel.